PKI 技术在敏感信息采集传输中的应用研究

摘　要：PKI 作为一种安全技术，已经深入到常规网络的各个层面，是现阶段网络信息安全问题的综合解决方案。通过分析 PKI 技术的组成、功能和特点，结合新华社的具体采编业务需求，阐述了如何运用 PKI/CA 技术通过数字加密和数字签名，确保信息保密性、完整性和不可抵赖性，从而解决新华社敏感信息采集传输业务中的关键技术难题。

关键词：PKI；信息安全；加密机制
中图分类号：TP309.2　　文献标识码：A
文章编号：1671-0134（2018）08-050-02　　DOI：10.19483/j.cnki.11-4653/n.2018.08.016

文 / 韩笑　李洁原

1.PKI 技术

1.1 PKI 的概念

PKI（Public Key Infrastructure）是一种遵循标准的利用公开密钥技术建立的提供信息安全服务的在线基础设施。它利用加密、数字签名、数字证书来保护应用、通信或者事务处理的安全。

PKI 必须具有权威认证机构 CA 在公钥加密技术基础上对证书的产生、管理、存储、分发和撤销进行管理的功能，包括实现这些功能的全部硬件、软件、人员、策略和规程，以及为 PKI 体系中的各成员提供全部的安全服务，如实现通信中各实体的身份认证、保证数据的完整、不可抵赖性和信息保密等。

1.2 PKI 的基本组成和功能

一个典型、完整、有效的 PKI 应用系统至少应具有以下部分：认证中心 CA（Certificate Authority）、注册机构 RA（Registration Authority）、证书库、密钥备份及恢复系统、证书撤销处理系统、客户端证书处理系统。提供的服务至少应具有以下功能：公钥密码证书管理、黑名单的发布和管理、密钥的备份和恢复、自动更新密钥、自动管理历史密钥、支持交叉认证。

1.3 PKI 的特点

PKI 作为一种安全技术，已经深入到常规网络的各个层面，是现阶段网络信息安全问题的综合解决方案。这从一个方面反映了 PKI 的天生的技术优势和强大生命力。

PKI 的特点主要有：

（1)公钥开放、私钥唯一，保障真实性和不可抵赖性。

（2）非对称密钥提供方便的机密性保护，既可以保证相互知道的实体间数据交换的机密性，又可以为不认识的实体之间的数据交互提供机密性保护支持。

（3）数字证书使密钥使用相对独立 ，不需要依靠其他在线支撑服务，除了依赖在线服务的限制，使业务拓展变得更加轻便与灵活。

（4）密钥管理更加安全，提供了撤销机制及其他服务，用来防止私钥泄露身份被非法使用。

（5）支持复杂网络化的信任结构，基于树状结构提供互信互认关系，为消除网络世界的信任孤岛提供了充足的技术保障。[2]

2.PKI 技术在敏感信息采集业务中的应用探索

参考报道是一项重要的报道形式，长期以来，记者外出采写的敏感素材稿上传问题因技术、安全等因素的制约未能得到较好的解决，尤其是在近几年的重大突发性事件报道中，该问题越来越突出，急需尽快解决。同时，随着在智库研究上的不断推进，记者在采集传输过程中对敏感信息的安全保密要求也越来越迫切。

由于敏感信息不能采用明文方式，通过采用基于 PKI/CA 技术的设计的敏感信息传输系统能够满足相关业务需求。PKI 基于 RSA 非对称加密算法，同时与对称加密算法混合使用，从而保证了信息的保密性和传输的高效性。[3]

2.1 设计理念

PKI 体系在敏感信息采集业务中主要有以下几部分：

（1）CA 认证中心。CA 认证中心负责证书的发放、撤销及证书发行后证书生命周期中各个环节的管理工作。

（2）注册机构 RA。RA 是数字证书注册的审批机构，是 CA 证书发放、管理的延伸。RA 也是用户和 CA 之间的接口，接受离线的证书申请，提供在线的证书申请服务。

（3）USB-key。USB-key 是具备硬件加密功能的终端认证与加密存储设备，在访问控制方面具有很强的安全保障，同时能够用于存储用户密钥、数字证书及业务数据，从而实现数据信息在采集终端上的身份认证和加密存储。

（4）信息加密算法。算法的复杂性和加解密密钥的长度决定了算法的安全性。算法越复杂，密钥长度越长，执行运算所需的时间也就越长，就越需要计算能力更强的芯片。系统采用符合国家密码管理局规定的密码设备

实现数据签名、验签、加密、解密等功能，搭配高处理性能的芯片，提供数据的机密性、可认证性、完整性和不可抵赖性以及数字信封等服务。

（5）数字证书。数字证书是 PKI 的核心数据结构，依赖证书上第三方的数字签名，用户可以离线的确认一个公钥的真实性。[1] 在实际应用中，证书认证系统需提供签发证书 / 证书注销列表的服务，用户身份注册、审核机构，并且承担整个证书认证系统的安全管理工作。

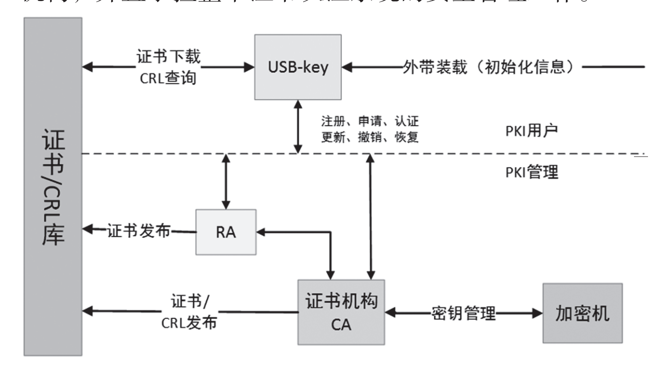


图 1　敏感信息采集业务中的 PKI 体系

基于PKI技术的敏感信息传输系统以终端发稿电脑、智能手机为稿件编辑载体，进行稿件的存储加密、传输加密、下载加密、强身份认证等安全加固。

身份认证加固：登录时采用双向身份鉴别，保证用户身份的合法性和安全性。

稿件存储加固：可进行本地稿件文字、图片加密存储，加密后的稿件数据用其他方式导出或第三方阅读器都无法打开。

传输链路加固：稿件在传输的链路中采用加密通道，避免稿件在传输中被篡改、丢失、恶意窃取等。

下载文稿加固：终端从总社服务器下载稿件文字和图片，加密存储在终端上。

2.2 CA 服务平台和签名及认证服务

在敏感信息传输系统中， CA 服务平台和签名及认证服务为安全的基础。CA 服务平台负责给用户签发数字证书，签名及认证服务用于验证用户的身份，并对客户端的加密数据进行解密处理。在实际应用中，CA 服务平台和签名认证服务采用现有的商密成熟产品方案。

CA 服务平台配置了 2 台密码机，可以为安全性、稳定性和设备性能要求较高的业务系统提供快速、高效的密码运算服务。CA 服务平台中的相关密钥均由密码机产生，根密钥也在该密码机的安全存储中，有效保证密钥的安全性。

签名及认证服务器系统为 CA 服务平台和敏感信息采集传输汇聚平台间的纽带和支柱，为应用系统提供全面的安全支撑，包括身份认证、数字签名验签、数据加解密及证书和证书状态查询等安全服务。

2.3 系统架构

敏感信息采集传输汇聚系统分为三部分：信息采集服务系统、安全管理系统、客户终端。

信息采集服务系统：主要负责提供数据内容服务（如上传、发布、浏览等），是信息资源应用与发布的执行者；结合密码技术、安全技术，提供敏感信息业务数据采集和传输。

安全管理系统：包括身份认证子系统、密码服务子系统、权限管理与访问控制子系统、监控与审计子系统等。其主要职责是完成敏感信息从产生、存储到传输、发布、应用，直至数据销毁全过程的数据访问与使用安全。

客户终端：是最终合法用户使用信息系统平台的认证密钥，也是终端数据加密与存储的密码设备。通过客户终端用户完成自身的身份认证与合法资源获取与本地数据的加密储存和管理。

2.4 业务实现

应用系统登录：系统为每个用户配备一个 USB–key 安全钥匙，提供用户身份鉴别和数据加解密存储与传输功能。用户必须插入自己的 USB–key，通过安全 PIN 码验证，方可启动客户端应用，访问系统资源，查看并使用加密文件。每个 key 代表一个操作用户的操作身份及权限，登录时根据 key 中的证书信息通过 CA 认证服务器进行证书有效性验证，并根据应用服务器进行用户权限信息核实获取。

加密和解密：记者和编辑的 PC 机、笔记本、智能手机上安装安全加固的信息采集客户端，配合终端密码安全设备进行稿件的采写、存储和传输。采写的稿件数据可经硬件加密后存储在指定的安全目录下（本地磁盘安全区或者移动安全密码终端设备）；传输过程中，数据都是以密文方式传送，稿件读入内存时通过 USB–key 进行解密，经 USB–key 回写于指定安全目录或加密后传输，做到“明文不落盘”。数据以密文形式传回后再对密文进行解密。

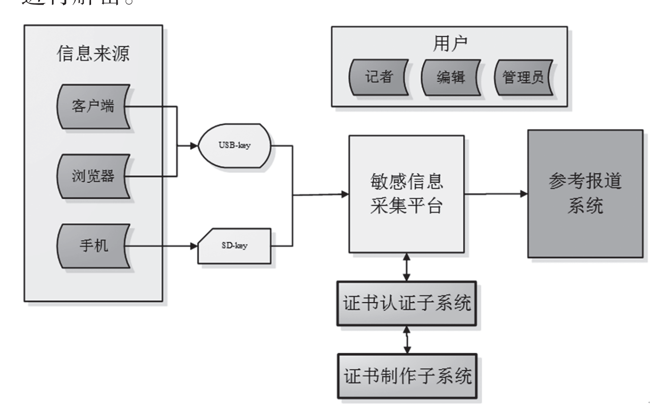


图 2　敏感信息采集业务流图

安全管理控制：总服务器端通过安全管理中心配置、分发、管理客户端安全钥匙，设定与下发终端安全策略；

（下转第69页）